UNIVERSIDADE FEDERAL DO PARANÁ

JESSICA GALDINO

OS CRIMES CIBERNÉTICOS NO AMBIENTE VIRTUAL

CURITIBA

2018

JESSICA GALDINO

OS CRIMES CIBERNÉTICOS NO AMBIENTE VIRTUAL

Projeto de conclusão de curso apresentado como requisito parcial à obtenção de grau de Bacharel em Gestão da Informação da Universidade Federal do Paraná.

Orientador: Prof. Dr José Simão de Paula Pinto.

CURITIBA

2018

RESUMO

Com a acelerada mudança na área da informática e com o grande uso da Internet como ferramenta de comunicação, os usuários estão expostos ao seu uso para atos ilícitos. Os tipos de crimes executados nessa área evoluíram com grande rapidez, porém as leis não conseguiram acompanhar essa rápida transformação. A imagem de anonimato transmitida pelas redes mundiais de computadores aumenta o interesse de indivíduos a praticar inúmeros tipos de crimes cibernéticos. Sendo assim, este estudo pautou-se em uma revisão dos principais tipos de crimes cometidos com o uso do computador e Internet, modos de prevenção, oferecendo sugestões de como agir a partir do momento em que seja vítima desse tipo de crime.

Palavras-Chave: Crimes virtuais. Crimes cibernéticos. Código Penal.

ABSTRACT

With the accelerated changes in the areas of informatics and the great use of the internet as a communication tool, users around the world are exposed to illicits acts. The variety of crimes in these areas evolved rapidly, however the law instruments could not keep up this transformation. The sense of anonymity that the World Wide Web transmit increase the interests of the individuals to commit ciber crimes. Thus, this study has been created based in the review of the main types of ciber crimes commited with the use of computers and internet, ways of prevention besides suggestions about how to act from the moment you became a viticm.

Key words: Virtual crimes. Ciber crimes. Criminal Code.

SUMÁRIO

1 INTRODUÇÃO

O avanço tecnológico cresce com grande força ao passar do tempo, os modelos de inovações são enormes, assim impactando no modo em que ocorrem as comunicações e distribuições de dados.

Com todo esse progresso tecnológico, a maneira de conduzir informações, ideias e expressões, aumentou de maneira significativa o modo em que as informações formuladas por um indivíduo podem ser espalhadas de maneira rápida para todo o mundo. A globalização e a evolução das tecnologias permitem que as informações sejam transmitidas em tempo real, trazendo um novo tipo de preocupação: A era dos crimes virtuais, também chamados de crimes cibernéticos ou informáticos. Podem ser considerados crimes virtuais aqueles “cometidos via Internet e se enquadram no nosso código penal, onde terá punições de acordo com cada caso”. Os crimes virtuais ocorrem com grande frequência. Dessa maneira, a segurança da informação é atualmente um problema sério e contínuo enfrentado por inúmeras pessoas, empresas e países.

Assim, surge a questão-problema: Como informar os usuários para que não sejam vítimas desses crimes virtuais, com relação a procedimentos e tipos de crimes? Além das leis que regem o nosso País, este trabalho propõe auxiliar os usuários, com os pilares da Gestão da Informação, nas suas tomadas de decisões ao expor suas informações em redes.

1.1 OBJETIVOS

O trabalho apresenta o objetivo geral e o desdobramento em objetivos específicos.

1.1.1 Objetivo Geral

Apresentar os tipos de crimes virtuais e o que fazer caso seja vitíma, com finalidade informacional.

---

[1] Disponível em: < (https://carmo311.jusbrasil.com.br/artigos/307607071/crimes-virtuais-conceito-e-seus-tipos).> Acesso em 06 dez 2018.

1.1.2 Objetivos Específicos

Os objetivos específicos do trabalho são:

a) Tipificar os tipos de crimes virtuais;
b) Apresentar alguns crimes virtuais conhecidos entre os usuários da internet;
c) Identificar os Artigos do Código penal para os crimes virtuais apresentados;
d) Identificar procedimentos das leis de proteção de dados
e) Melhores práticas;

1.2 JUSTIFICATIVA

Este trabalho é apoiado em pesquisas de cunho cientifico exploratório, baseado em três princípios da gestão da informação com seus principais pilares: coleta e organização dos dados, análise das informações coletas para elaboração da proposta do trabalho e disseminação de informações onde é apresentado o modelo de sugestão de prevenção para o usuário da Internet.

Além da carência de material de prevenção para usuários de redes, outra motivação para o desenvolvimento da pesquisa foi o interesse em descobrir como e por qual objetivo essas atitudes surgiram e cresceram de modo exponencial e abrangente nos últimos anos. A identificação de cada pilar dos crimes virtuais podem auxiliar os usuários em prevenções simples conseguindo assim, prevenir ou até mesmo reduzir uma possível taxa de ataques do cotidiano.

Do ponto de visto empírico pode-se supor que com a apresentação das leis referente os crimes, os usuários conhecem seus direitos e deveres diante a nação, para facilitar a convivência comunitária tornando-a mais justa, assim para os que descumprem as leis ocorram punições, principalmente para aqueles que agem com maldade ou beneficio próprio.

Os cibercrimes afetam diversos brasileiros juntamente com desvantagens morais, psicológicas e materiais. Os crimes também fazem parte do mundo empresarial, onde grande parte das organizações necessitam de prevenções com intensa segurança para proteger seu patrimônio e sua imagem.

2 LITERATURA PERTINENTE

Essa seção apresenta conceitos sobre Gestão da Informação, Crimes virtuais, Crimes cibernéticos, Código penal brasileiro, Segurança da informação e Tecnologia da informação e comunicação. O contexto é explorado por meio de levantamento de livros, artigos e informações extraídas de sites pertinentes ao tema selecionado. Importante ressaltar que os temas analisados visam trazer conhecimentos e entendimentos básicos após a disseminação da informação.

2.1 GESTÃO DA INFORMAÇÃO

Atualmente nada funciona sem um considerável número de informações como elemento que promove os acontecimentos sociais. Todos necessitam de informações para uma tomada de decisão seja, empresas privadas, públicas ou pessoas físicas e para que a informação seja utilizada de forma adequada e inteligente é indispensável que somente pessoas corretas tenham acesso a dados sigilosos ou pessoais. Segundo Drucker (1969, p. 264), “[...] o conhecimento é hoje o custo mais elevado, o principal investimento e o principal produto da economia avançada, bem como o meio de vida do maior grupo da população”. A informação hoje é a base da qual todo processo necessita, porém, de outra forma é significativo que a informação seja bem utilizada para trazer apenas benefícios.

Marchiori (2002) ressalta que a gestão da informação tem, por princípio, enfocar o indivíduo (grupos ou instituição) e suas “situações-problema” no âmbito de diferentes fluxos de informação, os quais necessitam de soluções criativas e custo/efetivas. Para Davenport (1998), a gestão da informação pode ser entendida como uma atividade organizada que considera a maneira como uma empresa obtém, distribui e usa informação e conhecimento.

Tarapanoff (2001), afirma que a informação deve ser gerida, sendo esta a base da administração dos recursos de informação, que consiste na visão integrada de todos os recursos envolvidos no ciclo de informação, que se constitui da seleção de dados, organização, catalogação e indexação, gerenciamento e recuperação da informação. A informação auxilia na compreensão de dados brutos, mas requer análise e compreensão humana, o que traz certa complexidade e deixa de se tornar uma interpretação simples de dados.

A gestão da informação é um método que consiste nas atividades de busca, identificação, classificação, processamento, armazenamento e disseminação de informações, sendo o objetivo principal tornar as informações úteis para um processo de tomada de decisão, seja ele pessoal, organizacional ou de estrutura cientifica. McGee e Prusak (1994) interpretam o processo de gestão da informação como um conjunto de tarefas, dentre elas:

- **Identificação das necessidades e requisitos de informação**: Compreender e identificar as necessidades informacionais.
- **Coleta de informação**: Coleta de dados a partir de fluxos formais ou informais,
- **Processamento, tratamento e armazenamento da informação**: Interpretação, tratamento e armazenamento de informações.
- **Distribuição e disseminação da informação**: Distribuição das informações ao usuário.
- **Análise e uso da informação**: Utilização das informações pelas pessoas.

É possível compreender o conceito de gestão da informação como um processo constante de processos informacionais que proporcionem por meio de identificação, coleta, armazenamento, distribuição e utilização das informações para tomadas de decisão ou para criação de produtos ou serviços.

2.2 O VALOR DA INFORMAÇÃO

A informação é um dos bens mais valorizados hoje em dia, ela é expansiva, quanto mais utilizada mais ela cresce. Com o decorrer do seu uso se torna mais completa e valiosa, porém, quanto mais sofisticada maior a possibilidade de que a informação “vaze” e traga prejuízos imensuráveis.

Atualmente existem inúmeras opções onde é citado que alguns produtos são insubstituíveis, mas para o mundo da informação ela pode substituir até pessoas. Dentro desse mundo a informação não é considerada uma troca, ela é apenas partilhada e enquanto a demanda por essa informação for pequena o seu valor pode

ser muito caro, mas como esse mundo exige uma atualização constante em apenas alguns dias ela pode virar sucata e já não ter o mesmo valor.

De acordo com Buckland (1991) é possível identificar três grupos distintos acerca do conceito de informação:

a) Informação como coisa: compreende registros, dados e objetos com algum valor informativo

b) Informação como conhecimento: entidade subjetiva, percepção, assimilação e apreensão particular de fatos e eventos. Processo que ocorre na mente do indivíduo.

c) Informação com processo: faz referência ao processo mediante o qual o sujeito se informa. O ato de informar de comunicar fatos e a partir daí estabelecer operações entre o mundo material e o imaterial.

Para Goulart (2004) mais do que nunca, a informação é a chave para a sobrevivência em nossa sociedade informatizada. Compreender sua natureza e significado é o primeiro passo para podermos controlá-la e utilizá-la para o progresso social e individual. A informação é o elemento que permite a transição e transformação do homem em sociedade, sendo a informação a representação do momento em que o homem delimita o pensamento e o molda para uma forma simbólica possível de ser apreendida e comunicada.

O termo informação constata que dentro da linguagem comum, ela é usada como sinônimo de mensagem, notícias, fatos, eventos e ideias os quais são obtidos e passados sucessivamente como conhecimento fazendo com que cada indivíduo defina o valor e importância da informação recepcionada. Sendo assim, o gestor da informação deve atentar a princípios de segurança da informação.

2.3 SEGURANÇA DA INFORMAÇÃO

A segurança da informação está diretamente ligada com proteção de um conjunto de informações, com a intenção de proteger e preservar o seu significado de valor para cada indivíduo ou organização, com características básicas como: confidencialidade, integridade, disponibilidade e autenticidade. (FERREIRA e ARAÚJO 2010, p.1) entendem que “Na sociedade da informação, ao mesmo tempo em que as informações são consideradas os principais patrimônios, estão também sob constante risco, como nunca estiveram antes”.

O conceito de segurança da informação adequa-se em todos os aspectos de proteção de informação e dados e não somente a sistemas computadorizados. Desse modo, pode também ser entendida como o processo de proteger informações de ameaças levando em conta três objetivos fundamentais, de acordo com Real (2005):

- Confiabilidade: garantia de que o acesso à informação é restrito aos seus usuários legítimos.

- Integridade: Garantia da criação legítima e da consistência da informação ao longo do ciclo de vida: em especial, prevenção contra criação ou alteração ou destruição não autorizada de dados e informações. O objetivo de autenticidade da informação é englobado pelo de integridade, quando se assume que este visa a garantir não só que as informações permaneçam completas e precisas, mas também que a informação capturada do ambiente externo tenha sua fidedignidade verificada e que a criada internamente seja produzida apenas por pessoas autorizadas e atribuída unicamente ao seu autor legítimo.

- Disponibilidade: Garantir de que a informação e os ativos associados estejam disponíveis para os usuários legítimos de forma oportuna.

A importância da informação cresce na mesma proporção em que a tecnologia passa a oferecer meios para tornar-se uma utilidade a um custo razoável. Em meio a tantas mudanças sociais no qual as informações pessoais e a privacidade se relacionam, qualquer análise feita a partir desse meio deve ser levada em consideração técnicas especificas para que não haja espaço para pequenos ou grandes erros, já que o controle da informação sempre foi um elemento fundamental na definição de poderes em uma sociedade.

2.3.1 SAFERNET BRASIL

Na descrição institucional do site SAFERNET BRASIL, a instituição foi fundada em dezembro 2005, é uma associação civil de direito privativo, com atuação nacional, sem fins lucrativos, políticos partidários, religioso ou racial.

Na época em que a SaferNet foi fundada o Brasil o país passava por grandes problemas relacionados ao uso indevido da Internet para a realização de crimes e violações contra os direitos humanos, e então a SaferNet Brasil concretizou-se como entidade de referência nacional para o defrontamento aos crimes e violações aos Direitos Humanos na Internet. Por sua capacidade de mobilização e articulações, produção de conteúdos e tecnologias para enfrentar os crimes cibernéticos, tem se firmado institucionalmente no plano nacional e internacional.

O objetivo da SaferNet é transfazer a internet para um ambiente ético e responsável, para que crianças, jovens e adultos consigam criar, desenvolver e ampliar suas relações sociais, com amplo conhecimento e exercitarem sua cidadania de forma segura e livre. Com base nos dados expostos no site SAFERNET, entre 2007 e 2017 foram 15.983 pessoas atendidas, 27 unidades da federação, 2.269 crianças, 1.751 pais e educadores e 11.963 outros adultos. Pode se ter uma breve análise das denúncias recebidas pelo SAFERNET no Anexo A, página 32 deste trabalho.

2.4 TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

As ideias de criação e desenvolvimento de rede deu-se a cibernética e também da relação com a informática interativa. Segundo ROSA (2000), em um dos seus estudos aponta que o movimento cibernético foi de grande influência para que a internet tivesse um amplo avanço. ROSA (2014) afirma que os avanços tecnológicos e as novas descobertas científicas trouxeram uma nova realidade para o ser humano, onde o espaço e a presença física não são mais fundamentais.

Operando programas, computadores, redes sociais e diversos outros sistemas que fazem parte da Tecnologia da Informação e Comunicação (TIC), os sinais criptografados por fibras óticas e ondas eletromagnéticas através dos canais de comunicação, permitem que as pessoas consigam estar em vários locais ao mesmo tempo. Rosa (2014) afirma que “é possível perceber o impacto social das atividades criminosas no espaço cibernético, está diretamente ligado ao crescimento do número de pessoas que passam a utilizar as novas tecnologias, sendo elas empresas privadas, órgãos governamentais ou pessoa física”.

No mundo globalizado as informações são disponibilizadas de forma excedida e inerente a elas, tornando-se necessário o apoio da TIC para processar essas

informações de maneira rápida e devido a essa explosão de informações disponibilizadas é necessário que os indivíduos desenvolvam consciência crítica sobre as informações apresentadas, analise sobre a relevância das informações e efetuem buscas para validação dos dados.

> MARCHESSOU (1997), afirma que excesso nas mídias, onde as performances tecnológicas e o consumo de informação submergem, “anestesiam” a capacidade de análise dessa informação e de reflexão tanto individual quanto social. Saturação e superabundância ameaçam o navegador da Internet que, como certas pesquisas mostram, não tira partido das riquezas de informação pertinente.

2.4.1 REDES SOCIAIS

A evolução tecnológica com o passar das últimas décadas tornou-se hoje um eficaz meio de comunicação. A internet tem demonstrado ser altamente dinâmica e conseguindo atingir cada vez mais um maior domínio de pessoas em todo o mundo, o desenvolvimento de tecnologias sofisticadas trouxeram a possibilidade de que pessoas de variadas partes do mundo se conectassem, constituindo assim uma rede global de comunicação.

Rede social é um sistema composto por diversas pessoas e organizações conectadas por inúmeros tipos de relações, que possuem objetivos e valores em comum, sendo sua conexão estabelecida por suas identidades. Levy (2002), explica que as comunidades virtuais são uma nova forma de fazer sociedade. Assim, não temos uma subsociedade, temos um novo filtro para a sociedade já existente.

As redes sociais podem atuar de de diversas maneiras e níveis, por exemplo, redes de relacionamento (Facebook, Instagram, Twitter, Baddo, youtube, MySpace) rede profissional (LinkedIn), redes com objetivo amoroso, espionagem e protestos, trazendo até mesmo a possibilidade de tornar alguns meios já muito utilizados a tornarem-se obsoletos, como por exemplo as chamadas eletrônicas. Todos os modelos padrões de redes sociais têm obtido importância e chamado a atenção com uma crescente frequência em toda a sociedade moderna. O principal ponto em comum de ambos os tipos de redes sociais é o compartilhamento de informações entre seus usuários, por objetivos em comum como: compartilhamento de informações, conhecimentos, interesses e curiosidades, essas redes sociais possuem o mesmo interesse, porém com objetivos diferentes, por exemplo: O

LinkedIn, possui o foco em praticar o networking aspirando ganhos profissionais, já outras redes como instagram e facebook possuem o foco em divulgações, laços com pessoas conhecidas, contato fácil com familiares, amigos e pessoas distantes.

O mundo de redes sociais online tem crescido juntamente com a internet, por conta das inúmeras atividades associadas a ela, como também tem aberto partido para “abrigo” dos criminosos que fazem uso desses recursos de diversas formas enfatizando sempre seu anonimato. Em consequência, os crimes desde o mais banal até os transnacionais utilizam-se dessas comunidades virtuais. Lamentavelmente os usuários destas comunidades se expõem além do normal e acabam abrindo brechas para que os ataques ocorram de modo constante. Segundo Moura (2006), a necessidade do indivíduo em se sentir parte de algo é o principal motivo pelo qual as pessoas buscam ingressar em uma rede social, pois a possibilidade de acesso a vida pessoal dos indivíduos aguça a curiosidade.

2.5 CRIMES VIRTUAIS E CIBERNÉTICOS

Os primeiros crimes virtuais iniciaram-se na década de 70 e grande parte era praticada por especialistas em informática, com o objetivo de quebrar o sistema de segurança das empresas. Hoje não sofremos mais com esse perfil específico para os crimes virtuais, os tempos mudaram e os responsáveis pela prática desses crimes também. Atualmente as pessoas que possuem conhecimentos não tão aprofundado, mas possuem acesso à internet podem realizar a prática de um crime virtual e essa categoria de crime tem ganhado forças no Brasil.

> Faria (2012) para designar as formas de comportamentos ilegais ou, de outro modo, prejudiciais à sociedade, que se realizam pela utilização de um computador, são usadas várias expressões, tais como: criminalidade de informática, infrações cometidas por meio de computador, crimes de computador, cyber crimes, computer crimes, computing crimes, delito informático, crimes virtuais, crimes eletrônicos ou, ainda, crimes digitais, crimes cibernéticos, infocrimes, crimes perpetrados pela Internet, entre outras nomenclaturas que devem surgir dia após dia no universo da informática.

Viana (2013) afirma que com o surgimento dos computadores a vida do ser humano tornou-se mais simples, atividades denominadas por grandes espaços e tempos, passaram a ser efetuados de forma rápida e prática, o computador mostra o

poder de armazenar e transformar informações, sob o controle de instruções predeterminadas.

Com a experiência da revolução industrial, a qual trouxe modificações aos traços do mundo moderno, mudou o modo de vida da população mundial e trouxe um avanço extremamente significativo na mudança do homem do campo para as cidades. As máquinas começaram a se desenvolver e os trabalhadores que antes faziam seus trabalhos de modo artesanal começaram a controlar máquinas e as fábricas começaram a produzir maiores quantidades, novas criações como os navios, fizeram com que a rotatividade das mercadorias replica-se e as matérias primas chegassem também de modo mais rápido as pessoas, e assim começaram a despertar mais inventores com a intenção de mudar a maneira que o mundo fosse visto. Grandes invenções surgiram, como por exemplo, telefone, luz elétrica, televisão, fotografia, entre tantas outras.

Segundo Morimoto (2006) o primeiro computador eletrônico desenvolvido foi o ENIAC (Electronic Numerical Integrator and Computer ou Computador e Integrador Numérico Eletrônico), pela solicitação do exército americano e custou na época 6 milhões de dólares, ocupava uma área de 180m² e funcionava por meio de 70 mil resistores, 18 mil válvulas e precisava de 200 mil watts de energia para funcionar. O computador demorou em torno de 3 anos para ser construído (1943-1946) e foi ligado apenas um ano depois de sua finalização.

Os primeiros discos removíveis foram os disquetes, nos anos de 1980 e em 20 anos era possível armazenar em cinco pequenos retângulos de plástico o que o RAMAC 305 fazia com 50 discos magnéticos e a partir de então a capacidade de armazenamento cresceu de modo significativo.

Em volta de todas essas invenções e descobertas surgiu a internet na década de 60 por volta de 1996 por meio de uma necessidade militar em meio à guerra fria, e trouxe a curiosidade de algumas universidades para desenvolver o ARPANET (Advanced Research Projects Administration – Administração de Projetos e Pesquisas Avançados).

A internet sendo uma rede de computadores integrada por redes menores que comunicam-se entre si assim como os computadores se comunicam através dos seus endereços de IP onde inúmeras informações são trocadas.

> “A internet vem modificando o comportamento humano, incentivando a paixão pelo conhecimento, educação e cultura. Isso, entretanto, não é de graça; vem acompanhado da inseparável e sempre (má) companhia criminosa: os criminosos digitais”. (KAMINSKI, 2003, p.28).

Segundo o site Avast (2017), *Hackers* e *Crackers* são conhecidos por terem habilidades e conhecimentos aprimorados em computadores e dispositivos móveis, porém o direcional de cada um é oposto. De modo geral, os *Hackers* são indivíduos que utilizam seus conhecimentos avançados de forma positiva obtendo soluções para problemas, desenvolvendo soluções para segurança e funcionalidades para computadores. Já os *Crackers*, utilizam seus conhecimentos de maneira indigna rompendo sistemas de segurança para obter vantagens financeiras, desenvolver vírus para computadores domésticos e empresariais, explorando as vulnerabilidades que encontram. As atividades desenvolvidas pelos *Crackers*, são identificadas como ilegais, e por isso, são denominados criminosos.

Souza e Volpe (2015) afirmam que alguns *hackers* destroem os arquivos ou unidades de discos inteiros das pessoas. Eles são chamados de *Crackers* ou *vândalos*. Alguns *hackers* novatos não se preocupam em aprender a tecnologia; eles apenas querem baixar as ferramentas dos *hackers* para entrar nos sistemas de computadores, esses são chamados de script kiddies. Os *hackers* mais experientes, com habilidades em programação, desenvolvem programas para *hackers* e os postam na Web e nos sistemas de bulletin board. Em seguida, temos os indivíduos que não têm nenhum interesse em tecnologia, mas que usam o computador apenas como uma ferramenta que os ajudam a roubar dinheiro bens ou serviços.

O crime cibernético é uma ação praticada por *Crackers* que consistem na transmissão de vírus, invasão de sistemas, aplicativos e sites, esse tipo de crime traz em geral grandes prejuízos infectando e danificando redes empresariais, dados sigilosos, dados pessoais, portais governamentais, sites e sistemas. O ato é totalmente ilegal e é considerado um crime informático. Esse crime refere-se a todos os delitos cometidos utilizando computadores ou internet seja por uma rede pública, privada ou doméstica, os interesses são inúmeros e variam de acordo com o objetivo do infrator, assim como as maneiras em que o crime é realizado também são incontáveis, podendo ter o objetivo apenas de atingir um usuário, diversos usuários ou até mesmo um sistema de rede pública completo. A rede, que liga mais de 35 milhões de computadores em todo o mundo, é um dos caminhos prediletos

para as invasões. Segundo pesquisa realizada pelo CDN GoCache a lista dos dez países com maior taxa de cyber ataques são: China, EUA, Turquia, Rússia, Taiwan, Brasil, Romênia, Índia, Itália e Hungria. O Brasil é indicado como o sexto país com maior taxa de ataques mesmo não acreditando que 100% dos atos são de fato registrados oficialmente. Heitor Shimizu e Ricardo B. Setti (1995) concluem que “o destaque do Brasil no progressivo uso da rede mundial de internet tem animado os interessados em invadir sistemas”.

Com a grande quantidade de diversos tipos de informações em redes de modo disponível a inúmeras pessoas com acesso à internet e quando disponível de forma legal pelo usuário e quando não disponível pelo usuário são alvo de buscas por “usuários” que procuram nas redes brechas para os crimes, conhecidos como Crimes Virtuais.

Com o passar dos anos a tecnologia teve avanços imensuráveis, empresas e pessoas começaram a utilizar o computador como modo de criar, armazenar, enviar, transferir dados e ter acesso a inúmeros conteúdos e então também foram criados programas para facilitar suas inúmeras funcionalidades.

A internet passou a ser utilizada de forma comercial no Brasil, em dezembro de 1994, seu objetivo era facilitar a comunicação entre pessoas, empresas e países, melhorando as relações de consumo e aprendizado. Mas com os benefícios da internet, vieram também várias espécies de delitos.

Alguns usuários dessas ferramentas também passaram a usufruir da internet de maneira inadequada, acessando banco de dados indevidamente com a intenção de causar danos secundários.

> Segundo PRUSAK (2001, p.1002) “à medida que o acesso à informação se expande dramaticamente, de forma que as pessoas possam ter acesso a quase toda a informação de que elas necessitam a qualquer hora e em qualquer lugar, o valor das habilidades cognitivas ainda não replicadas pelo sílicio aumente”a.

As pessoas não obrigatoriamente realizavam crimes de informática com intenção financeira, mas em grande parte por prazer e para comprovar suas habilidades, provocando destruições, corrupções e até mesmo inutilização de programas e dados de computadores, sendo capaz de causar extremos prejuízos.

Assim os crimes virtuais podem ser definidos como às condutas de acesso não autorizado a sistemas informáticos, ações de destruição nos sistemas informáticos, interceptação de comunicações, alterações de dados, descriminação entre outros. (VIDAL 2015, p.7) conclui que “pode se chegar à conclusão de que crimes virtuais são todas as condutas típicas, antijurídicas e culpáveis praticadas contra ou com a utilização dos sistemas da informática”. “Desde sua origem o homem busca desenvolver máquinas e ferramentas para que auxiliem no seu dia a dia tornando suas tarefas mais fáceis e simples” (VIANA, 2013, p.11).

2.5.1 TIPIFICAÇÕES DOS CRIMES CIBERNÉTICOS

Segundo FARIA (2012), a criação do código penal brasileiro ocorreu em 1940 pela Lei 2848, nessa época não se pensava em “era da informação” a qual deu início em meados de 1970 e teve seu progresso apenas em 1990 com constante evolução até os dias atuais.

Nessa época o Brasil não possuía leis especificas e os artigos do Código Penal também não se enquadravam aos crimes praticados pela internet, e nenhuma informação que enunciasse a respeito da tipificação de tais crimes. No entanto, atualmente não é a falta de leis específicas que impedem as pessoas de responder por seus atos no mundo virtual.

2.5.2 LEGISLAÇÃO APLICÁVEL

Cyberbullying: Surgiu com o aparecimento da Internet e a popularização das redes sociais.

> Segundo Silva (2010) Trata-se da migração para o meio virtual da conduta chamada em inglês “bullying” que corresponde a um conjunto de atitudes de violência física e/ou psicológica, de caráter intencional e repetitivo, praticado por um ou mais agressores contra uma ou mais vítimas que se encontram impossibilitadas de se defender.

No ambiente virtual, a violência surge através de intimidações, humilhações, ameaças, deboches mensagens ou fotografias alteradas e postadas nas redes para

serem visualizadas por incontáveis números de pessoas, causando danos de maneira muitas vezes irreversíveis.

Racismo: Quando utiliza-se nomenclaturas referente a raça, cor, etnia, religião, origem, gênero ou condição financeira.

> Até o final dos anos 1960, a maioria dos dicionários e livros escolares definiam [o racismo] como uma doutrina, dogma, ideologia, ou conjunto de crenças. O núcleo dessa doutrina era de que a raça determinava a cultura, e daí derivam as crenças na superioridade racial. Nos anos 1970, a palavra foi usada em sentido ampliado para incorporar práticas e atitudes, assim como crenças; nesse sentido, racismo passa a denotar todo o complexo de fatores que produzem discriminação racial e, algumas vezes, frouxamente, designa também aqueles fatores que produzem desvantagens raciais. (Banton & Miles, 1994, p. 276)

Art. 140 - Quando se ofende uma ou mais vítimas, por meio de elementos referentes à raça, cor, etnia, religião e origem.

Racismo - Previsto na Lei específica, 7.716/1989. É crime contra a coletividade e não contra uma pessoa ou grupo específico.

Crimes contra honra na internet: Envolvem ameaça, calunia, difamação, injúria e falsa identidade. Honra é denominada com a qualidade de um indivíduo físicas, morais e intelectuais, fazendo-se respeitada no meio social e também a qual diz respeito a sua autoestima.

Recorrente os crimes de calúnia, difamação e injúria, previsto no código penal do **Art. 138 a 145**.

Assédio: Constitui-se em perseguição inconveniente de forma persistente que possui como alvo uma pessoa ou grupo específico atingindo sua liberdade, paz e dignidade.

Art. 216-A. Constranger alguém com o intuito de obter vantagem ou favorecimento sexual, prevalecendo-se o agente da sua condição de superior hierárquico ou ascendência inerentes ao exercício de emprego, cargo ou função.

Espionagem: Quando ocorre interceptação, decodificação, tradução e análise de mensagens por terceiro.

Art. 143 Conseguir, para o fim de espionagem militar, notícia, informação ou documento, cujo sigilo seja de interesse da segurança externa do Brasil.

Art. 144 Revelar notícia, informação ou documento, cujo sigilo seja de interesse da segurança externa do Brasil.

Pornografia infantil: Para que o crime seja definido é necessário que o executor tenha a finalidade de expor ao público, ou comercializar o objeto material do crime, não sendo necessário que alguém tenha acesso ao conteúdo para que o crime venha a ser empregar, é necessário somente a disponibilização do conteúdo e a oportunidade de que alguém venha a ter acesso ao mesmo.

Art. 240 do Estatuto da Criança e do Adolescente - Produzir ou dirigir representação teatral, televisiva ou película cinematográfica, utilizando-se de criança ou adolescente em cena de sexo explícito ou pornográfica.

Art. 241 do Estatuto da Criança e do Adolescente - Fotografar ou publicar cena e sexo explícito ou pornográfia envolvendo criança ou adolescente

Terrorismo: É denominado quando utilizado como forma de manipulação psicológica e demonstração de forças de ataques militares. Essa propaganda pode ser direcionada a diversos públicos: inimigos, demonstração de poder e ameaça e efetivação da execução de ataques.

Lei 7170 – Art. 20 CP - Devastar, saquear, extorquir, roubar, sequestrar, manter em cárcere privado, incendiar, depredar, provocar explosão, praticar atentado pessoal ou atos de terrorismo, por inconformismo político ou para obtenção de fundos destinados à manutenção de organizações políticas clandestinas ou subversivas.

Intimidação: Obrigar ou forçar alguém a praticar algo.

Art. 146 - Constranger alguém, mediante violência ou grave ameaça, ou depois de lhe haver reduzido, por qualquer outro meio, a capacidade de resistência, a não fazer o que a lei permite, ou a fazer o que ela não manda.

Chantagem/extorsão: Coagir alguém de modo que a amedronte para que seu comportamento seja de determinada e de forma que a faça cumprir todos os propósitos de quem a chantageia.

Art. 158 - Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa.

Estelionato: A aplicação do estelionato na internet ocorre quando o cracker atua para manter a vítima em erro, e assim, obter vantagem ilícita, para si ou para outrem.

Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.

Falsificação de documento particular: Falsificar no todo ou em parte documento particular ou alterar documento reconhecido como verdadeiro.

Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro.

Falsificação de cartão: Clonar e usufruir de cartões de crédito ou débito sem o consentimento do proprietário.

Art. 155 – Subtrair, para si ou para outrem, coisa alheia móvel. § 4º II - com abuso de confiança, ou mediante fraude, escalada ou destreza.

2.5.3 LEI CAROLINA DIECKMANN (LEI Nº12.737/12 de 30 de novembro de 2012)

A lei 12.737/12 foi sancionada em 30 de novembro de 2012 pela ex presidente Dilma Rousseff, a qual se fez alterações no Código Penal Brasileiro. A legislação é oriunda do projeto de Lei 2793/2011 apresentado em 29 de novembro de 2011 pelo deputado Paulo Teixeira (PT-SP), em comparação com outros projetos sobre delitos informáticos que as leis apreciavam.

A nova lei acrescentou dois artigos ao código penal, Art. 154-A e Art. 154-B:

- **Invasão de dispositivo informático**

Art.154-A: Invadir dispositivo informático alheio, conectado ou não à rede de computadores mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

- **Ação penal**

Art. 154-B: Somente se procede mediante representação, salvo se o crime for cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Além dos dois atuais artigos inseridos na lei do Código Penal, os crimes de injuria, calúnia e difamação cometidos em redes sociais já eram tipificados pelo Código Penal.

2.5.4 MARCO CÍVIL DA INTERNET (LEI Nª 12.965 de 23 de abril de 2014)

No ano de 2014 a Lei 12.965/14 foi sancionada com o objetivo de estabelecer princípios, garantias, direitos e deveres para uso na Internet no Brasil, determinando ainda as de atuação da União, dos Estados Unidos, Distrito Federal e dos Municípios em relação à matéria. A Lei traz dispositivos, garantias do direito de defesa dos consumidores que utilizam a Internet para adquirir produtos e serviços, como também regulariza a comercialização de empresas que utilizam a Internet como meio de negócios, assegurando a concorrência e iniciativa livre.

2.6 INCIDÊNCIA DE CRIMES VIRTUAIS

Por conta do seu acesso infinito, a internet tem como posicionamento atualmente o maior meio de comunicação de todo o mundo, adquirindo constantemente novos usuários que buscam usufruir de seus benefícios sendo ele, negócios, lazer e obtenção de bens e serviços.

Com todo o avanço tecnológico continuo e desordenado, diversos criminosos passaram a utilizar a internet para efetuar crimes virtuais, como o estelionato, calunia, furto e racismo, com a ideia de que suas identidades não fossem identificadas pelos delitos cometidos.

Podemos citar os crimes virtuais mais conhecidos como: Vírus de computador, programas e códigos maliciosos, os roubos de informações, fraudes de dados e acessos não autorizados. Dentro dos crimes citados entram os crimes mistos ou comuns que usam a internet como instrumento de bullying, intimidação, chantagem, calúnia, assédio, extorsão, espionagem, estelionato, pornografia infantil, terrorismo e clonagem.

Fabrízio Rosa demonstra sua opinião com o seguinte posicionamento:

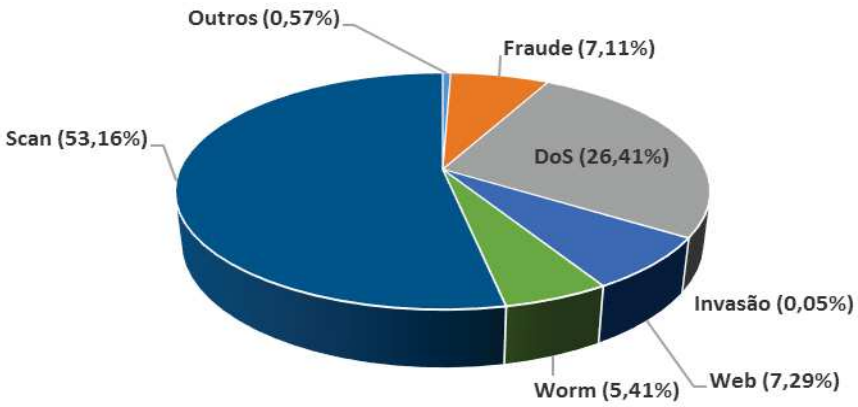
> “Com a expansão do uso de computadores e com a difusão da internet, tem-se notado, ultimamente, que o homem está se utilizando dessas

> facilidades para cometer atos ilícitos, potencializando, cada vez mais, esses abusos cometidos na rede. Como todos os recursos de disponibilidade do ser humano, a informática e a telecomunicação não são utilizadas apenas para agregar valor. O abuso (desvalor), cometido por via, ou com assistência dos meios eletrônicos não tem fronteiras" (ROSA, 2005, p. 3).

Além dos crimes comuns e mistos também é possível citar o crime puro onde se enquadra o ataque de negação de serviços, que possui como objetivo fazer com que um servidor ou computador ganhe uma grande sobrecarga para que sistemas específicos fiquem inacessíveis como: buscador de páginas e compra de um produto específico e suas maiores vítimas são os servidores de web onde os crackers tornam as páginas hospedadas indisponíveis na web sem visar a extração de informações confidencias ou modificações de conteúdos armazenados.

Conforme o gráfico 1, é possível visualizar o percentual de incidentes reportados ao CERT.br no ano de 2017.

Gráfico 1 – Incidentes por tipo de ataque reportados ao CERT.br



Legenda:

- **worm**: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
- **dos** (DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- **invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
- **web**: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
- **scan**: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente

utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

- **fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
- **outros**: notificações de incidentes que não se enquadram nas categorias anteriores.

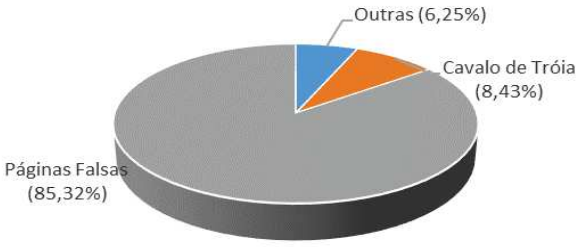
Fonte: Cert.br

Os crimes virtuais também são conhecidos pelas organizações públicas e privadas. As violações dentro de grandes empresas crescem de maneira exponencial a cada ano e torna-se necessário grandes investimentos para proteção de seus dados e informações. No Site Globo.com Moreira (2018) afirma que os custos de crimes cibernéticos podem alcançar 8 trilhões de dólares nos próximos cinco anos e os registros contra a violação tecnológica dobram desde 2012.

Os ataques são cada vez mais sofisticados e profissionais, direcionado para bens valiosos das companhias como dados, informações e dinheiro. Os crackers são focados em falhas humanas para capturar dados e atuam de qualquer lugar do mundo, em geral usando redes falsas para que seja possível alterar constantemente seu endereço de IP, trazendo dificuldades e empecilhos para o grupo de policiais responsáveis pela investigação do crime.

No Site CERT.br foi divulgado o percentual dos incidentes por tentativas de fraudes em 2017, conforme apresentação do gráfico 2.

Gráfico 2 – Incidentes por tentativas de fraudes reportados ao CERT.br



Legenda, por CERT.br

- **Cavalos de Tróia**: Tentativas de fraude com objetivos financeiros envolvendo o uso de cavalos de tróia.
- **Páginas Falsas**: Tentativas de fraude com objetivos financeiros envolvendo o uso de páginas falsas.
- **Outras**: Outras tentativas de fraude.

Fonte: CERT.br

Todos os usuários, independentemente do nível social, cultural e de escolaridade estão vulneráveis a sofrer algum tipo de crime virtual. Quanto maior a exposição de informações pessoais, maior o risco de sofrer um golpe.

Segundo o Site Globo.com (2018) a rede social Facebook sofrou um ataque em setembro de 2018 onde os crackers tiveram acesso à 29 milhões de contas dentro da rede e roubaram nomes, números de telefones, e-mails, gênero, localidade, idioma, religião, status de relacionamento, data de nascimento, dispositivos utilizados para acessar o Facebook, local de trabalho e os últimos dez locais onde os usuários estiveram ou foram marcados. Assim tornou-se difícil se defender das invasões digitais, mas existem medidas a serem tomadas caso haja a ocorrência sobre o assunto.

Por ser um novo gênero de crime, onde não há um entendimento consolidado e concreto a respeito do método probatório e das medidas necessárias à conservação de provas obtidas, se faz necessário para que o profissional de tecnologia de informação, autoridade policial e os demais operadores do direito apliquem a maior proteção possível para a preservação das evidências. Primeiramente, o administrador de sistema ou de redes, ou qualquer profissional de tecnologia de informação pode apresentar queixa as autoridades quando certificar-se de uma ocorrência de crime digital. A notícia do crime, que é o conhecimento pela autoridade, de um fato aparentemente criminoso deve ser apresentada no momento da queixa, que é quando qualquer pessoa pode comunicar o fato delituoso à autoridade policial, dando conjuntura à instauração de inquérito. É o que faculta o Código de Processo Penal:

> Art. 5º - Nos crimes de ação pública o inquérito policial será iniciado: (...) § 3º - Qualquer pessoa do povo que tiver conhecimento da existência de infração penal em que caiba ação pública poderá, verbalmente ou por escrito, comunicá-la à autoridade policial, e esta, verificada a procedência das informações, mandará instaurar inquérito.

3 METODOLOGIA

Esta seção apresenta a classificação da pesquisa, a análise do cenário bem como o tratamento dos dados coletados.

3.1 CARACTERIZAÇÃO DA PESQUISA

De acordo com Gil (2008), a caracterização da pesquisa é realizada com base em métodos e técnicas sob o ponto de vista de sua finalidade, abordagem, objetivos e procedimentos.

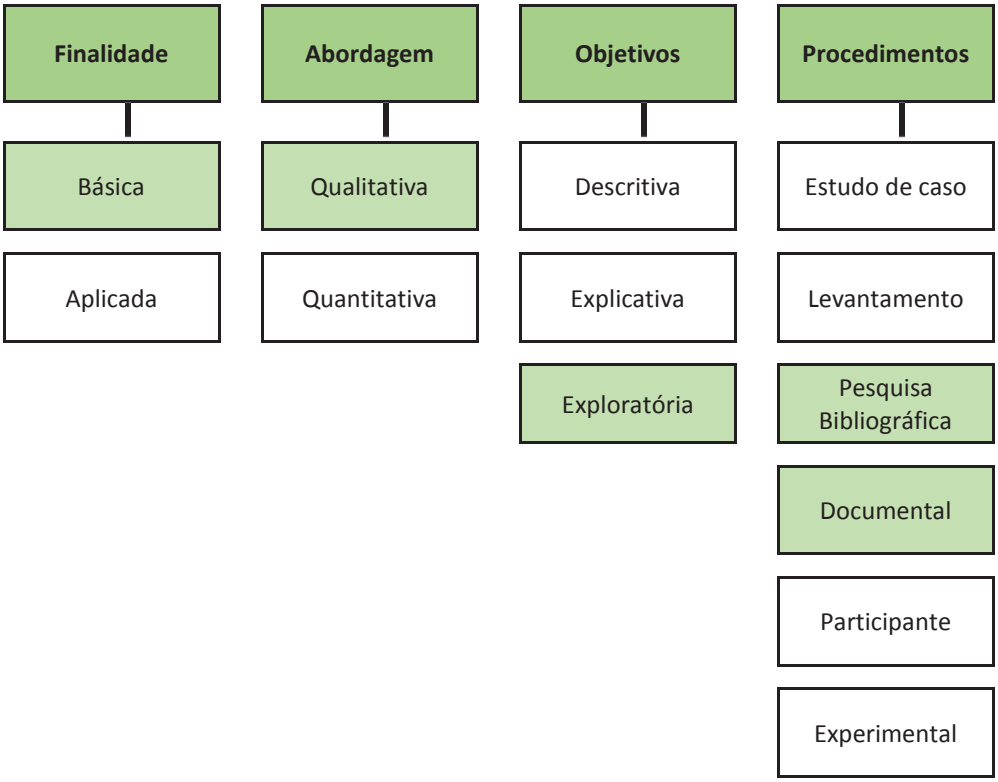
A finalidade desta pesquisa apresentada classificou-se como básica com o objetivo de gerar conhecimento aos usuários vulneráveis a algum tipo de ataque no mundo virtual, Gil (2008) afirma que uma pesquisa básica deve ser motivada pela curiosidade, e suas descobertas devem ser divulgadas para a comunidade. Sua abordagem é designada como qualitativa, MINAYO (2012) cita que pesquisas qualitativas são aquelas capazes de transmitir informações concisas e coerentes, e este trabalho tem como foco a transmissão de informações sucintas sobre a trajetória dos crimes virtuais.

Enquanto procedimento, este trabalho realizou-se por meio de uma pesquisa bibliográfica e documental que se utiliza de materiais já publicados, constituído de livros, artigos e atualmente com material disponibilizado na Internet.

Em relação aos objetivos, a presente pesquisa é classificada como exploratória, pois, segundo Gil (2002), possui o objetivo a exploração de um assunto por meio da aproximação de fatos, o que se realiza através da identificação, do acesso e uso de materiais informacionais – fontes.

A figura 1 demonstra a caracterização de pesquisa de acordo com as citações e explicações realizadas.

Figura 1 – Caracterização da pesquisa



FONTE: Elaborado pela autora (2018).

3.2 COLETA E TRATAMENTO DE DADOS

Para o desenvolvimento da pesquisa foi utilizado como instrumento de coleta de dados, livros, artigos acadêmicos, legislações pertinentes e informações coletadas através de sites de forma em que fosse possível demonstrar e analisar os crimes com maior índice de ocorrência atualmente, junto as leis que trazem a oportunidade de defesa para usuários que sofreram ou sofrem ataques virtuais. A primeira fonte de informação considerada para análise e mensuração do tema foi o site SAFERNET, que disponibiliza percentuais e informações explicativas sobre os crimes com maior ocorrência no Brasil, onde foi possível ter uma visão ampla do material para estudo e após essa análise as pesquisas nos conteúdos bibliográficos foram aprofundadas para melhor estruturar o trabalho e análises de artigos

específicos da legislação foram feitos para entender sua aplicação para os crimes virtuais.

As coletas iniciaram em fevereiro de 2018 com término em novembro do mesmo ano, dentro desse período por meio das informações analisadas foi possível defini-lá como uma apresentação descritiva para todas as informações coletadas, assim como sua análise definida como interpretativa com colocações originais da própria autora.

O resultado esperado deste trabalho é a apresentação de um quadro de maneira ilustrativa onde seja possível para o usuário sua visualização com sugestões de possíveis formas e maneiras de prevenção e informações simples do cotidiano em que os tornam mais vulneráveis aos crimes cibernéticos.

4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Após as análises realizadas para identificar um padrão entre os crimes e efetuar o tratamento das informações para criação do quadro “classificação dos crimes”, foi possível identificar que dentro de um crime denominado como principal ou chave pode-se caracterizar vários crimes e artigos que facultam dentro dele através da classificação de crimes por puro, misto e comum.

4.1 CLASSIFICAÇÃO

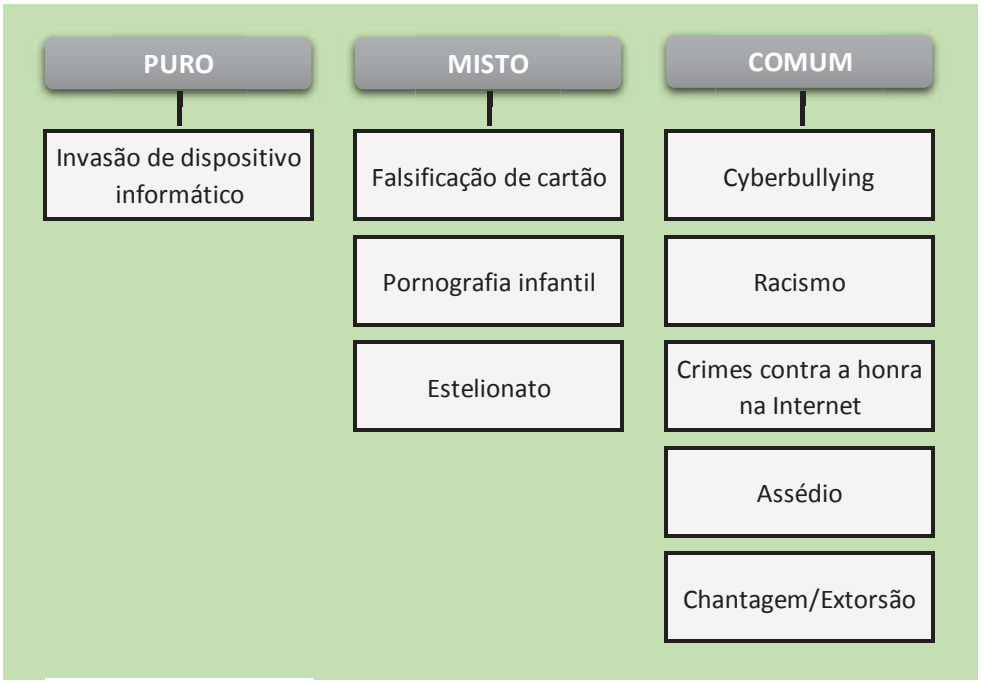
É possível classificar os crimes virtuais em três categorias, segundo Silvia (2003), Viana (2013) e Maggio (2013):

- **Crime virtual puro**: Compreende em qualquer conduta ilícita, a qual atenta o hardware ou o software, sistemas obtidos no computador e meios de armazenagem externo, ou seja, atingindo a parte física, técnica e seus componentes. Segundo Silvia (2003), os crimes informáticos puros, são aqueles provenientes do uso da informática, em que este é utilizado como meio para fim específico pelo agente do crime. Nesse momento pode-se identificar a ação dos *crackers*, que são as pessoas com profundos conhecimentos computacionais e que se utilizam desse conhecimento para ganhar algum tipo de benefício ilícito ou até mesmo apenas por vandalismo.
- **Crime virtual misto**: Utiliza a intenet para conduzir condutas ilícitas, e com objetivo diferente do crime virtual puro, como por exemplo transações ilegais de valores de contas correntes, utilizando-se do computador para alcançar o resultado da vantagem ilegal e o uso do computador para este tipo de crime é primordial. Segundo Viana (2013), são delitos derivados da invasão de dispositivos informáticos, dada a importância do bem jurídico protegido diverso da inviolabilidade dos dados informáticos.
- **Crime virtual comum**: Condutas em que se utiliza a internet como instrumento para realizar delitos que se enquadram no Código Penal e para este caso o sistema de informática não é essencial, o que possibilita o uso de outras ferramentas para o crime virtual comum. Por exemplo, se antes, a

> pornografia infantil era disseminada apenas por vídeos e fotografias, hoje é comum o acesso via home-pages. Maggio (2013), classifica o crime virtual comum aquele que pode ser praticado por qualquer pessoa.

Com base nos conceitos apresentados anteriormente, percebe-se que os crimes virtuais mais conhecidos foram classificados para melhor entendimento do usuário, conforme a imagem abaixo. Para efetuar essa divisão entre as categorias dos crimes, foram analisados os principais crimes virtuais citados nas páginas 18 à 21, com o objetivo de identificar alguns padrões entre eles para influenciar no tratamento dessas informações e assim ser possível realizar a criação de um quadro de modo objetivo para melhor visualização, conforme a figura 2.

Figura 2 – Classificação dos crimes.



FONTE: Elaborado pela autora (2018), baseado em Silvia (2003) Viana (2013) e, Maggio (2013).

4.2 RESULTADO

Foi possível realizar a classificação dos principais crimes baseados em suas categorias: puro, misto e comum. A partir dessa classificação foi permitido criar tópicos com informações para o usuário como: Tipo de crime, onde eles ocorrem, o que fazer caso seja vítima, por que seguir as orientações citadas, possíveis consequências para o usuário e os artigos que se enquadram em cada crime citado.

A seguir encontram-se as classificações criadas.

Crime Puro e misto

Crime: Furto de dados

Onde: Sites de compras e sites atrativos

O que fazer?

- Busque sempre informações sobre o site antes de realizar uma compra para checar sua veracidade;
- Faça buscas para verificar a opinião de outros possíveis clientes;
- Verifique se o telefone disponível no site é realmente verdadeiro;
- Certifique-se de que o modo de pagamento proposto é de fato seguro;
- Não clicar em anúncios de promoções chamativas;
- Não instalar aplicativos desconhecidos em celulares ou computadores;
- Caso seja vítima desse tipo de crime, entrar em contato imediatamente com o banco para notificar sobre a compra indevida, solicitar o cancelamento do cartão e também entrar em contato com a Polícia para registrar o boletim de ocorrência;

Por que seguir as instruções acima?

- Para esse tipo de crime, cabe destacar que é o modo mais fácil dos criminosos conseguirem ter acesso aos dados armanezados em computadores ou celulares como: fotos, arquivos pessoais, contas bancárias e acesso as informações de cartão de crédito e debito.

Possíveis consequências ao usuário:

- Todas as informações furtadas podem ser usadas para extorsão da vítima.

Artigos do Código Penal que se enquadram:

- Art 171 CP - Estelionato;

- Art 298 CP - Falsificação de documento particular;
- Art 155 CP - Falsificação de cartão;
- Art 154 CP – Invação de dispositivo informático;

Crime comum

Crime: Calúnia, difamação e injúria

Onde: Redes sociais

O que fazer?

- Caso seja vítima desse tipo de crime, é necessário salvar todas as provas de modo impresso ou print screen e ir até a delegacia para registrar o boletim de ocorrência, e em alguns casos é possível também mover ação por danos morais.

Por que seguir as indicações acima?

- Apenas com esses cuidados é possível punir os responsáveis por esses atos.

Possíveis consequências ao usuário:

- Exposição negativa do usuário, podendo acarretar em difamações ainda maiores, trazendo transtornos psicológicos.

Artigos do Código Penal que se enquadram:

- Art 140CP - Racismo;
- Art 138 a 145 CP - Crimes contra a honra na Internet;
- Art 216A CP - Assédio;
- Art 240 e 241 do Estatuto da criança - Pornografia Infantil;
- Art 158 CP - Chantagem/Extorsão;

Crime misto

Crime: Pedofilia

Onde: Internet em geral

O que fazer ?

- Ir até a delegacia para registrar o boletim de ocorrência;
- Não compartilhar com amigos ou companheiros de relacionamento suas fotos íntimas;

- Não compartilhar vídeos com imagens íntimas ou atos sexuais;
- Caso o conteúdo seja disponibilizado em uma página de Internet, deve ser feito print screen da página ou impressão para que seja possível remover o material da internet;
- Não marcar encontros com pessoas anônimas conhecidas via internet.

Por que seguir as indicações acima?

- Para garantir a segurança dos menores de 18 anos e também para proteger a exposição da vida intíma.

Possíveis consequências ao usuário:

- Trauma psicológico.

Artigos do Código Penal que se enquadram:

- Art 247 – Pedofilia da Lei nº8.069/90 – Estatuto da Criança e do Adolescente.
- Art 158 CP - Chantagem

Crime Puro

Crime: Utilização de softwares falsos

Onde: Na instalação de software em computadores ou aplicativos em celulares e tablets.

O que fazer?

- Não instalar programas desconhecidos;
- Pesquisar a confiabilidade do programa ou app;
- Fazer o uso de antivírus no computador, tablets e celulares;

Por que seguir as indicações acima?

- Para evitar problemas futuros e garantir a segurança dos dados armazenados nesses dispositivos.

Possíveis consequências para o usuário:

- Os invasores por trás dos softwares falsos podem conseguir ter acesso a todas as informações do seu dispositivo seja ele computador, tablet ou celular, tornando o usuário vulnerável a futuras extorsões ou prejuízos financeiros.

Artigos do Código Penal que se enquadram:

- Art 12 – Crimes contra software – Pirataria da lei nº 9.609/98

Crime Misto e Comum

Crime: Criação de perfis falsos

Onde: Redes sociais

O que fazer?

- Para pessoa física: Aceitar convite em redes sociais apenas de pessoas que você conhece realmente.
- Caso desconfie de um perfil fake, utilize as ferramentas disponibilizadas nas redes sociais para fazer a denúncia da página ou perfil.
- Não iniciar ou manter contato com pessoas desconhecidas via internet;
- Para pessoa Jurídica: Certifique-se sempre de realizar o input de informações seguras e com opções de teste para certificação dessas informações, assim evitando que outras páginas se passem por um perfil original divulgando fake News.

Por que seguir as indicações acima?

- Para garantir a segurança de seus dados pessoais e para impedir A divulgação de propagandas ou promoções indevidas de um determinado comércio.

Possíveis consequências para o usuário:

- Pessoa física: Disponibilização de informações pessoais para desconhecidos;
- Pessoa Jurídica: Prejuízos financeiros e fake News;

Artigos do Código Penal que se enquadram:

- Art 370CP - Falsa identidade

Através da classificação, foi possível identificar que, de maneira geral, são inúmeros os crimes virtuais. Porém, conseguimos ter visibilidade daqueles que mais afetam os usuários da Internet em seu cotidiano e com base nesse instrumento foi realizado a análise para melhor estruturar essa cadeia dos crimes virtuais e mostrar ao usuário que dentro de um crime especifíco existem diversos outros crimes e com isso pode-se ter o conhecimento de como se prevenir, quais ferramentas utilizar ou de que modo agir caso seja vitíma de um desses supostos ataques e também disponibilizar o conhecimento de que existem artigos dentro do código penal

brasileiro que foram adequados para punir pessoas que agem de má fé no mundo virtual.

5 CONSIDERAÇÕES FINAIS

A informação é de suma importância para um cidadão, principalmente seus dados pessoais ou financeiros. Com a questão dos dados se manterem em rede, a proteção contra roubo precisa se manter mesmo que não-físicos. Os ambientes estão interconectados assim os dados ficam expostos por este motivo devemos minimizar os riscos.

Por meio da pesquisa exploratória observou-se que os crimes virtuais já existem a muitos anos, mas ele se tornou mais evidente nos dias atuais, devido ao fácil acesso que temos a todas as tecnologias nos dias de hoje. Antigamente os crimes virtuais existiam, mas suas finalidades e objetivos eram outros, em geral esse tipo de crime ocorria para espionagem ou investigação e atualmente os crimes de informática ocorrem por diversos e inúmeros motivos, desde o mau caráter e vândalos virtuais até os mais robustos onde se tem acesso a informações sigilosas de pessoas, empresas ou órgãos públicos.

Diante dos dados obtidos foi verificado que os crimes informáticos praticados com e contra o computador passam a ser uma preocupação social e por mais que não exista um código específico que supra todos os crimes virtuais temos uma legislação adaptada para esses crimes onde é possível punir pessoas que exercem esses atos.

Desta forma, este trabalho colabora na questão informacional relativa a cibercrimes.

5.1 SUSTENTAÇÃO DOS OBJETIVOS PROPOSTOS

Perante aos objetivos estabelecidos deste trabalho, foi possível alcançar todos os objetivos específicos.

O primeiro objetivo específico: Tipificar os tipos de crimes virtuais;

O segundo objetivo específico: Apresentar alguns crimes virtuais conhecidos entre os usuários da internet;

O terceiro objetivo epecífico: Identificar os artigos do Código Penal para os crimes virtuais apresentados;

O quarto objetivo específico: Identificar procedimentos das leis de proteção de dados e melhores práticas;

Para encerrar este trabalho acadêmico respondendo a questão-problema: Como informar os usuários para que não sejam vitímas desses crimes virtuais? No trabalho foram indicadas algumas formas para que os usuários possam se prevenir de alguns crimes específicos cujo eles são os mais populares entre o nosso cotidiano e também mostrar que diversos dos crimes que ocorrem pela Internet podem ser punidos por artigos que contemplam o nosso Código Penal e as denúncias podem ocorrer não somente em delegacias especializadas, mas também em delegacia comum.

5.2 LIMITAÇÕES DO TRABALHO

Este item trabalha os aspectos de grande importância que não houve condições de ser abordado, devido aos conteúdos específicos não serem parte do curso de Gestão da Informação.

a) As técnicas utilizadas pelos *crackers* para invação de sistemas e computadores com a intenção de coletar informações sigilosas e pessoais.
b) Explicação e detalhes dos artigos do Código Penal.

5.3 RECOMENDAÇÕES PARA TRABALHOS FUTUROS

Diante das limitações apresentadas para este trabalho, destaca-se entre as sugestões para trabalhos futuros a análise aprofundada do Código Penal Brasileiro e o entendimento sistêmico de todo o processo relacionado ao cibercrime de um *cracker*.

Por fim, será interessante verificar os resultados das análises detalhadas geradas dentro dos aspectos computacionais e judiciais.

REFERÊNCIAS

AVAST. **Hacker** Disponível em: <https://www.avast.com/pt-br/c-hacker>. Acesso em: 29 mai.2018.

BANTON, M. & MILES, R. 1994 **"Racism", in CASHMORE, E.,** ***Dictionary of Race and Ethnic Relations*****,** 3. ed., London/New York, Routledge.

BRASIL. **Lei 12.965 de 23 de abril de 2014.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 02 mai. 2018.

BRASIL. **Lei 12.737 de 30 de novembro de 2012.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 04 mai. 2018.

BUCKLAND, M. **Information as thing**. Journal of the American Society of Information Science, v.42, n. 5, p. 351-360, jun. 1991.

Cert.BR. Disponível em: https://www.cert.br/. Acesso em: 01 dez 2018.

DAVENPORT, T. H. **Ecologia da Informação**. 6.ed. São Paulo: Futura, 1998.

DRUCKER, P. F. **The age of discontinuity**: guidelines to our changing society. New York: Harper and Row, 1969.

FARIA, Matheus Afonso de. **O Problema da tipificação dos crimes informáticos.** Rio Grande: Revista âmbito Jurídico, 2012. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=11275>. Acesso em: 18 maio 2018.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de segurança da informação:** Guia prático para elaboração e implementação. 2. ed. Rio de Janeiro: Ciência Moderna Ltda., 2008.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4 ed. São Paulo. Atlas, 2002.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

GOCACHE. **Veja os 10 países do mundo com maior número de hackers e crimes cibernéticos.** Disponível em <https://www.gocache.com.br/seguranca/dez-paises-com-mais-ataques-de-hackers/>. Acesso em: 15 mai. 2018.

GOULART. **Precisamos definir esse termo**. Disponível em < http://observatoriodaimprensa.com.br/diretorio-academico/precisamos-definir-esse-termo/>. Acesso em: 18 out. 2018.

GLOBO.COM. **Os crimes cibernéticos podem custar US$ 8 tri**. Disponível em: <http://www.valor.com.br/empresas/5271249/os-crimes-ciberneticos-podem-custar-us-8-tri>. Acesso em 07 mai.2018.

GLOBO.COM. **Facebook diz que hackers roubaram dados de 29 milhões de usuários.** Disponível em https://g1.globo.com/economia/tecnologia/noticia/2018/10/12/facebook-diz-que-hackers-roubaram-dados-de-29-milhoes-de-usuarios.ghtml>. Acesso em 09 nov.2018.

IBMEXC. **Pesquisa básica e pesquisa aplicada**. Disponível em: < http://ibmec.org.br/geral/pesquisa-basica-e-pesquisa-aplicada/>. Acesso em: 07 mai. 2018.

KAMINSKI, Omar. **Internet Legal: O direito na tecnologia da informação**. 1ed. Curitiba: Juruá, 2003.

LEVY, P. **Cyberdemocratie**. Paris: Odile Jacob, 2002.

LOUREIRO NETO, José da Silva. **Direito Penal Militar.** 5. ed. São Paulo: Atlas S.A., 2010.

MAGGIO, Vicente de Paula Rodrigues. **Novo crime**: invasão de dispositivo informático - CP, Art. 154-A. Disponível em: http://vicentemaggio.jusbrasil.com.br/artigos/121942478/novo-crime-invasao-de-dispositivo-informatico-cp-art-154-a. Acesso em: 01 nov. 2018.

MARCHESSOU, François. Estratégias, Contextos, Instrumentos, Fórmulas: a contribuição da tecnologia educativa ao Ensino Aberto e à Distância. **Revista Tecnologia Educacional** – V. 25 (139), Nov./Dez. 1997 – p. 6 a 15

MARCHIORI, P. Z. **A ciência e a gestão da informação: compatibilidades no espaço profissional**. Ciência da Informação. Brasília, v.31, n.2, p. 72-79, maio/ago.2002.

MCGEE, J. V.; PRUSAK, L. **Gerenciamento estratégico da informação:** aumente a competitividade e a eficiência de sua empresa utilizando a informação como uma ferramenta estratégica. Rio de Janeiro: Campus, 1994.

MINAYO, Maria Cecília de Souza. Análise qualitativa: teoria, passos e fidedignidade. **Ciênc. saúde coletiva** , Rio de Janeiro, v. 17, n. 3, p. 621-626, mar. 2012. Disponível em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-81232012000300007&lng=en&nrm=iso>. Acesso em 08 de setembro de 2018. http://dx.doi.org/10.1590/S1413-81232012000300007.

MORIMOTO, Carlos e. **ENIAC:** A História da informática (Parte 6: Sistemas embarcados e supercomputadores). São Paulo: Guia do Hardware, 2011. Disponível em: <https://www.hardware.com.br/guias/historia-informatica/eniac.html>. Acesso em: 20 maio 2018.

MOURA, Patrícia do Nascimento. **O Marketing de Mídias Sociais e a Influência no Comportamento do Consumidor**. Disponível em http://pt.scrib

d.com/doc/20716918/O-MARKETING-DE-MIDIAS-SOCIAIS-E-A-INFLUENCIA-NO-COMPORTAMENTO-DO-CONSUMIDOR>. Acesso em 08 maio 2018.

PLANALTO. **Decreto-lei Nº 2.848, de 7 de dezembro de 1940.** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em 05 mai. 2018.

PRUSAK, L. **Where did knowledge management came from?** IBM Systems Journal, Armonk, v. 40, n. 4, p. 1002-1007, 2001.

REAL, Adriana. **SEGURANÇA DA INFORMAÇÃO:** Princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas S.A., 2005.

ROSA, Antônio Machuco. **As origens históricas da Internet: uma comparação com a origem dos meios clássicos de comunicação ponto a ponto.** Estudos em Comunicação, Porto, n. 11, p.89-116, 30 out. 2014.

ROSA, Fabrízio. **Crimes de Informática**. 2º ed. Campinas: Bookseller, 2005.

SAFERNET. **Institucional**. Disponível em: <http://new.safernet.org.br/content/institucional>. Acesso em: 31 mai. 2018.

SHIMIZU, Heitor; SETTI, Ricardo. **Tem boi na linha: hackers os espiões cibernéticos**. Super Interessante, São Paulo, out. 1995. Disponível em:< http://super.abril.com.br/tecnologia/tem-boi-linha-hackers-espioes-ciberneticos-441127.shtml>. Acesso em: 15 maio 2018.

SILVA, A. B. B. **Bullying**: mentes perigosas nas escolas. Rio de Janeiro: Objetiva, 2010.

SILVA, Rita de Cássia Lopes da. **Direito Penal e sistema informático**. Revista dos Tribunais. São Paulo, v.4, 2003.

SOUZA, Henry Leones de; VOLPE, Fernando Cassilhas. **Da ausência de legislação específica para os crimes virtuais**. Alta Floresta: Revista Juridicare, 2015. Disponível em: <http://www.egov.ufsc.br:8080/portal/sites/default/files/da_ausencia_de_legislacao_especifica_para_os_crimes_virtuais.pdf>. Acesso em: 02 mai 2018.

TARAPANOFF, K. **Inteligência organizacional e competitiva**. Brasília: Editora Universidade de Brasília, 2001.

VIANA, Túlio. **Crimes informáticos.** Belo Horizonte: Fórum, 2013.

ANEXO A – DENÚNCIAS FEITAS AO SAFERNET 2015 À 2017

A demonstração do quadro abaixo é feita com base nos números disponibilizados no site SAFERNET, dos atendimentos realizados via chat ou e-mail entre 2015 e 2017.

Denúncias	2015		2016		2017		Total			Média	
	Feminino	Masculino	Feminino	Masculino	Feminino	Masculino	Total	Total Feminino	Total masculino	Médica F	Média M
Aliciamento sexual infantil online	54	19	33	26	34	13	179	121	58	68%	32%
Ciberbullying/ofensa	173	92	202	110	242	117	936	617	319	66%	34%
Conteúdos impróprios/Violentos	160	75	80	48	72	44	479	312	167	65%	35%
Controle parental	4	6	6	3	3		22	13	9	59%	41%
Cyberstalking	3	5	11	2	16	29	66	30	36	45%	55%
Encontros virtuais	38	16	31	12	33	11	141	102	39	72%	28%
Fraudes/Golpes/email falso	41	48	44	65	65	75	338	150	188	44%	56%
Orientações gerais	6	3	3	4	0	0	16	9	7	56%	44%
Outros	86	123	96	98	94	101	598	276	322	46%	54%
Pornografia infantil	26	20	33	18	36	51	184	95	89	52%	48%
Problemas com compras online	22	42	23	31	20	40	178	65	113	37%	63%
Problemas com dados pessoais	107	96	119	154	128	171	775	354	421	46%	54%
Sexting/Exposição íntima	232	79	202	98	204	85	900	638	262	71%	29%
Situações off-line	83	27	62	38	708	251	1169	853	316	73%	27%
Solicitação de material/Palestras	49	27	64	25	61	20	246	174	72	71%	29%
Uso excessivo	1	3	1	2	5	2	14	7	7	50%	50%

FONTE: Elaborado pela autora (2018).